UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: **Collins et al.**
Serial No: **09/328,726**
Filing Date: October 26, 1998

Docket No: 20206.25 (PT-TA410Cont1)
Group Art Unit: 2766
Examiner: Leaning, J.

#11

For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

Assistant Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL FOR INFORMATION DISCLOSURE STATEMENT

Enclosed for filing in the above-identified application is:

1) Information Disclosure Statement with attached Form PTO-1449 and copies of cited references; and

The Commissioner is authorized to charge any required fees, or credit any overpayment to Deposit Account No. 02-3964.

Respectfully submitted,

Dated: September 27, 2000

Leah Sherry
Reg. No.43,918

OPPENHEIMER WOLFF & DONNELLY LLP
1400 Page Mill Road
Palo Alto, CA 94304
Telephone: 650-320-4000
Facsimile: 650-320-4100

CERTIFICATE OF MAILING (37 CFR 1.8a))

I hereby certify that this paper (along with any referred to as being attached or enclosed) is being deposited on the date shown below, with the U.S. Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C., 20231.

Date: September 27, 2000

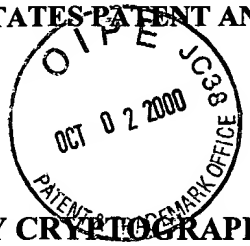
Leah Sherry

[illegible] 00000065 09320726

240.00 OP

PATENT

UNITED STATES PATENT AND TRADEMARK OFFICE



Inventor: **Collins et al.**
Serial No: **09/328,726**
Filing Date: October 26, 1998

Docket No: 20206.25 (PT-TA410Cont1)
Group Art Unit: 2766
Examiner: Leaning, J.

For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

Assistant Commissioner for Patents
Washington, D.C. 20231

INFORMATION DISCLOSURE STATEMENT

Applicant submits herewith the references listed on the attached form PTO-1449 of which Applicant is aware which are believed to be material to the examination of this application and in respect of which there may be a duty to disclose in accordance with 37 CFR 1.56.

The filing of this information disclosure statement shall not be construed as a representation that a search has been made (37 CFR 1.97(g)), nor as an admission that the information cited is, or is considered to be, material to patent ability, nor an admission that no other material information exists.

The filing of this information disclosure statement shall not be construed as an admission against interest in any manner. Notice of January 9, 1992, 1135 O.G. 13-25, at 25.

Respectfully submitted,

DATE: September 27, 2000

Leah Sherry
Reg. No: 43,918

OPPENHEIMER WOLFF & DONNELLY LLP
1400 Page Mill Road
Palo Alto, CA 94304
Tel: (650) 320-4000
Fax: (650) 320-4100

CERTIFICATE OF MAILING (37 CFR 1.8a))

I hereby certify that this paper (along with any referred to as being attached or enclosed) is being deposited on the date shown below, with the U.S. Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C., 20231.

Date: September 27, 2000

Leah Sherry

(Information Disclosure Statement)

SV:107379.01
09272000/13:06/2C06.25

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTY DOCKET NO.	SERIAL NO.
	20206-25	09/328,726
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	APPLICANT	
	Collins	
	FILING DATE	GROUP
	October 26, 1998	2766

U. S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	NAME	CLASS	SUBCLASS	TRANSLATION YES NO

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

	AB		*IEEE 1994 Electronics Letters Online No: 19941450 "Using four-prime RSA in which some of the bits are specified"* S. A. Vanstone and R. J. Zuccherat – Electronics Letters 8th December 1994 Vol 30, No. 24, pp. 2118, 2119.
	AC		*RSA '98 Presentation – F. Levy-dit-Vehel – January 98 "Stuffing An RSA Into The Smallest 68HC05", pp. 1-14.*
	AD		*Generating a Product of Three Primes With an Unknown Factorization,* Dan Boneh and Jeremy Horwitz, Computer Science Department, Stanford University.
	AE		*ChipCenter: The Web's Definitive Electronics Resource – "Compaq Computer Corporation – WebScan :Press Release" (4/11/00)*
	AF		*Newell Public Relations, Hong Kong – "RSA Security teams with Compaq to provide high-speed cryptography breakthrough for manufacturers of wireless and embedded devices" (April 19, 2000)*
	AG		*Compaq News via WebLibrary – "New RSA BSAFE Crypto-C Encryption Software Offers up to 500 Percent Performance Gains for E-Commerce, Secure E-Mail and Other Applications"* PR News Wire via DowVision (September 6, 2000).
	AH		*Compaq News via WebLibrary – "RSA Security Releases RSA Encryption Algorithm into Public Domain"* PR News Wire via DowVision (September 6, 2000).
	AI		*RSA Security – RSA BSAFE* - Wireless Transport Layer Security for C (8/31/2000).*
	AJ		*CyberLaw Presents: The RSA Algorithm & The RSA Patent – "Using the RSA Algorithm for Encryption and Digital Signatures: Can You Encrypt, Decrypt, Sign and Verify without Infringing the RSA Patent?"* Patrick J. Flinn and James M. Jordan III*; (c) 1997 Alston & Bird LLP (July 9, 1997).
	AK		*RSA Laboratories / Bulletin 13 (April 2000) "A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths"* Robert D. Silverman, RSA Laboratories
	AL		*1982 International Symposium on Information Theory;* Les Arcs, France (June 21-25, 1982).
	AM		*Lecture Notes in Computer Science (Edited by G. Goos and J. Hartmanis) – "Advances in Cryptology – CRYPTO '86" Proceedings*
	AN		*"An Introduction to Fast Generation of Large Prime Numbers"* by C. Couvreur and J. J. Quisquater; Phillips J. Res. 37, 231-264, 1982
	AO		*"A Method for Obtaining Digital Signatures and Public Key Cryposystems"* R. L. Rivest, A. Shamir, and L. Adelman, MIT Laboratory for Computer Science and Department of Mathematics
	AP		*MIT/LCS/TR-212 – "Digitalized Signatures and Public-Key Functions As Intractable As Factorization"* Michael O. Rabin (January 1979) Massachusetts Institute of Technology Laboratory for Computer Science.
	AQ		*Permutation Polynomials in RSA-Cryptosystems* Rudolf Lidl and Winfried B. Müller; Department of Mathematics, University of Tasmania, Hobart Australia 7001 and Institut für Mathematik, Universität Klagenfurt, A-9020 Klagenfurt, Austria
	AR		*PKCS #1: RSA Encryption Standart – An RSA Laboratories Technical Note, Version 1.5, Revised November 1, 1993*

	AS		*High-Speed RSa Implementation* Cetin Kaya Koc, RSA Laboratories RSA Data Security, Inc., 100 Marine Parkway, Suite 500, Redwood City, CA 94065-1031; Copyright © RSA Laboratories Version 2.0 – November 1994

EXAMINER	DATE CONSIDERED
EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	